

İNFORMASIYA TƏHLÜKƏSİZLİYİ MƏDƏNİYYƏTİNİN CƏMİYYƏTDƏ FORMALAŞMASI: MÖVCUD SIXINTILAR VƏ PERSPEKTİVLƏR

DOI: <https://doi.org/10.71447/2413-7235-2025-1-52>

Gülçin E. Hüseynli

Azərbaycan Dövlət İqtisad Universiteti, magistrant

E-mail: huseynli.gulchin.elmir.2024@unec.edu.az

ORCID: 0009-0008-1911-0302

Xülasə

Məqalədə informasiya təhlükəsizliyi mədəniyyətinin müasir cəmiyyətdə rolu və onun formalaşması araşdırılmışdır. İnformasiya təhlükəsizliyi artıq yalnız texniki tədbirlərlə məhdudlaşmır, eyni zamanda sosial, hüquqi və iqtisadi aspektləri də əhatə edir. Rəqəmsal texnologiyaların sürətlə inkişafı və internetin geniş yayılması şəxsi və korporativ məlumatların qorunmasını daha da aktuallaşdırmışdır. Məqalədə vurğulanır ki, cəmiyyətin maarifləndirilməsi, hüquqi çərçivələrin təkmilləşdirilməsi və texnoloji infrastrukturların inkişafı informasiya təhlükəsizliyi mədəniyyətinin formalaşmasında əsas amillərdir. Müasir dövrdə kibertəhlükələr fərdi və kollektiv səviyyədə ciddi risklər yaradır. COVID-19 pandemiyası dövründə məsafədən işin sürətlə tətbiqi nəticəsində fişinq və zərərli proqram hücumları artmış, fərdi məlumatların sızma riski yüksəlmişdir. Azərbaycanın nümunəsində dövlət və özəl sektor birgə tədbirlər həyata keçirərək milli kibertəhlükəsizlik ekosistemini gücləndirmişdir. Eyni zamanda, “e-Estonia” və Yaponiya kimi ölkələrin təcrübəsi göstərir ki, informasiya təhlükəsizliyi yalnız texniki deyil, həm də təhsil, maarifləndirmə və sosial yanaşmalarla möhkəmləndirilə bilər. Məqalədə beynəlxalq təcrübələr və ölkəmizdə görülən tədbirlər - milli strategiyalar, hüquqi bazanın gücləndirilməsi, “Ağıllı şəhər” və “Ağıllı kənd” layihələri, kibertəhlükəsizlik təlimləri və qabaqlayıcı texnoloji həllər – nəzərdən keçirilmişdir. Təklif olunan tövsiyələr arasında maarifləndirmənin genişləndirilməsi, hüquqi və idarəetmə mexanizmlərinin möhkəmləndirilməsi, dövlət-özəl sektor əməkdaşlığının artırılması və sünİ intellekt əsasında innovativ kibermüdafiə sistemlərinin tətbiqi xüsusi yer tutur. Məqalə nəticəsində vurğulanır ki, informasiya təhlükəsizliyi mədəniyyətinin inkişafı yalnız texnologiya ilə deyil, həm də cəmiyyətin hər bir üzvünün bilik və məsuliyyətli davranışı ilə təmin edilə bilər, bu da milli və fərdi maraqların qorunmasını gücləndirir.

Açar sözlər: *informasiya təhlükəsizliyi, rəqəmsal savadlılıq, əməkdaşlıq, kibermədəniyyət, təhsil.*

THE FORMATION OF INFORMATION SECURITY CULTURE IN SOCIETY: CURRENT CHALLENGES AND PROSPECTS

Gulchin E. Huseynli

Master's Student

Azerbaijan State University of Economics (UNEC)

E-mail: huseynli.gulchin.elmir.2024@unec.edu.az

ORCID: 0009-0008-1911-0302

Abstract

The article explores the role of information security culture in modern society and its formation. Information security is no longer limited to technical measures but also covers social, legal, and economic aspects. The rapid development of digital technologies and the widespread use of the internet have made the protection of personal and corporate data increasingly relevant. The article emphasizes that public awareness, improvement of legal frameworks, and development of technological infrastructure are key factors in shaping information security culture. In today's world, cyber threats create serious risks on both individual and collective levels. During the COVID-19 pandemic, the rise of remote work caused phishing and malware attacks to increase, raising the risk of personal data leaks. In Azerbaijan, joint initiatives by the state and private sector have strengthened the national cybersecurity ecosystem. At the same time, the experiences of countries such as "e-Estonia" and Japan show that information security can be reinforced not only by technical means but also through education, awareness, and social approaches. The article reviews international practices and measures taken in Azerbaijan, including national strategies, a stronger legal base, "Smart City" and "Smart Village" projects, cybersecurity training, and preventive technological solutions. Recommendations include expanding awareness campaigns, strengthening legal and governance mechanisms, enhancing public-private cooperation, and applying AI-based innovative cyber defense systems. Ultimately, the article stresses that developing information security culture depends not only on technology but also on the knowledge and responsible behavior of every member of society, ensuring the protection of both national and individual interests.

Keywords: *information security, digital literacy, cooperation, cyber culture, education.*

ФОРМИРОВАНИЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЩЕСТВЕ: СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Гюльчин Э. Гусейнли

магистрант, Азербайджанский государственный экономический университет

E-mail: huseynli.gulchin.elmir.2024@unec.edu.az

ORCID: 0009-0008-1911-0302

Резюме

В статье рассматривается роль культуры информационной безопасности в современном обществе и процесс её формирования. Информационная безопасность уже не ограничивается лишь техническими мерами, но также охватывает социальные, правовые и экономические аспекты. Быстрое развитие цифровых технологий и широкое использование интернета делают защиту личных и корпоративных данных особенно актуальной. Подчёркивается, что ключевыми факторами формирования культуры информационной безопасности являются повышение осведомлённости общества, совершенствование правовой базы и развитие технологической инфраструктуры. В современном мире киберугрозы создают серьёзные риски как на индивидуальном, так и на коллективном уровнях. В период пандемии COVID-19 рост удалённой работы вызвал увеличение фишинговых атак и распространение вредоносных программ, что усилило риск утечки персональных данных. В Азербайджане совместные инициативы государства и частного сектора способствовали укреплению национальной экосистемы кибербезопасности. Опыт таких стран, как «e-Estonia» и Япония, показывает, что информационная безопасность должна обеспечиваться не только техническими средствами, но и через образование, просвещение и социальные подходы. В

статье анализируются международный опыт и меры, предпринятые в Азербайджане: национальные стратегии, укрепление правовой базы, проекты «Умный город» и «Умная деревня», тренинги по кибербезопасности и внедрение превентивных технологических решений. В числе рекомендаций — расширение просветительской работы, совершенствование правовых и управленческих механизмов, развитие сотрудничества государства и частного сектора, а также применение инновационных систем киберзащиты на основе искусственного интеллекта. В заключение подчёркивается, что развитие культуры информационной безопасности зависит не только от технологий, но и от знаний и ответственного поведения каждого члена общества, что укрепляет защиту как национальных, так и личных интересов.

Ключевые слова: *информационная безопасность, цифровая грамотность, сотрудничество, киберкультура, образование.*

GİRİŞ

Müasir dövrdə informasiya təhlükəsizliyi yalnız texniki tədbirlərlə məhdudlaşmır, eyni zamanda cəmiyyətin mədəniyyət səviyyəsi ilə də sıx bağlıdır. İnformasiya təhlükəsizliyi mədəniyyəti fərdlərin və təşkilatların məlumatları qorumaq üçün göstərdiyi davranış və yanaşmaların məcmusudur. Rəqəmsal texnologiyaların sürətli inkişafı və internetin geniş yayılması nəticəsində şəxsi və korporativ məlumatların qorunması daha da aktuallaşmışdır.

Rəqəmsallaşma prosesinin sürətlənməsi ilə informasiya təhlükəsizliyi yalnız texniki məsələ deyil, həm də sosial və iqtisadi sabitliyin qorunmasında strateji rol oynamağa başlamışdır. Dünya Bankının 2023-cü il hesabatında qeyd olunur ki, “kibertəhlükəsizlik rəqəmsal transformasiyanın əsas dayəğıdır və onun zəifliyi iqtisadi və sosial sabitliyə birbaşa təsir göstərir.” (World Bank, 2023)

Bununla belə, cəmiyyətin informasiya təhlükəsizliyi sahəsində maarifləndirilməsi və bu mədəniyyətin formalaşması bir sıra çətinliklərlə üzləşir. İnsanların kibertəhlükələrə qarşı kifayət qədər məlumatlı olmaması, təşkilatların bu sahədə lazımi tədbirləri görməməsi və hüquqi çərçivələrin tam formalaşmaması mövcud problemlər sırasındadır. Digər tərəfdən, yeni texnologiyalardan və informasiyadan insanların düşüncəsini, davranışını manipulyasiya etmək, onların mənəvi-psixoloji sağlamlığına zərər vurmaq üçün də istifadə edilir. Bununla əlaqədar, texnosferada baş verən köklü dəyişikliklər insanın təfəkküründə və davranışında da dəyişikliklərin edilməsini tələb edir. İnformasiya məkanında şəxsiyyətə təsir sahəsindəki situasiyanın ciddiliyini, bu prosesi izah etmək üçün istifadə edilən terminologiya da sübut edir: informasiya müharibəsi, informasiya silahı, informasiya terrorizmi, informasiya təxribatı, informasiya killeri. Bütün bu problemlər cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılmasının zəruriliyini meydana çıxarır.

Bu məqalədə informasiya təhlükəsizliyi mədəniyyətinin cəmiyyətdə formalaşması ilə bağlı mövcud sıxıntılar və bu sahədə inkişaf perspektivləri araşdırılacaqdır. Məqsəd, bu sahədə maarifləndirmənin artırılması və effektiv strategiyaların tətbiq edilməsi üçün tövsiyələr təqdim etməkdir.

ƏDƏBİYYAT İCMALI VƏ METODOLOJİ YANAŞMA

Bu iş, informasiya təhlükəsizliyi mədəniyyətinin cəmiyyətdə necə formalaşdığını və bu prosesin qarşısında duran mövcud sıxıntıları özündə əks etdirir. Son dövrlərdə, cəmiyyətin informasiya təhlükəsizliyinə yanaşmasında maarifləndirmə, təhlükəsizlik mədəniyyəti və etika məsələlərinin rolu artmışdır. Beynəlxalq təşkilatlar və ekspert rəyləri, məlumat təhlükəsizliyi mədəniyyətinin inkişafında cəmiyyətin davranışlarının və hüquqi çərçivələrin vacibliyini vurğulayır. Ədəbiyyat, sosial mühəndislik, insan amili və texnoloji yeniliklər kimi sahələrdə mövcud boşluqları və çətinlikləri özündə əks etdirmişdir. Beynəlxalq hesabatlarla əsasən, məlumat təhlükəsizliyi sahəsində maarifləndirmə və qanunvericilik tədbirlərinin təkmilləşdirilməsi zəruridir.

Bu işdə informasiya təhlükəsizliyi mədəniyyətinin cəmiyyətdə formalaşması mövzusunda müqayisəli təhlil aparılmış, fərqli ölkələrdəki təcrübələr müqayisə edilərək, informasiya təhlükəsizliyi mədəniyyəti və onun inkişafı barədə ümumi nəticələr çıxarılmışdır.

TƏHLİL VƏ QIYMƏTLƏNDİRMƏ

İnformasiya təhlükəsizliyi mədəniyyəti - bir fərdin, təşkilatın və ya cəmiyyətin məlumatların qorunmasına dair doğru düşüncə tərz, davranış formaları və münasibətləri sistemli şəkildə mənimsəməsi və gündəlik fəaliyyətində tətbiq etməsi deməkdir.

Informasiya təhlükəsizliyi mədəniyyətinin strukturuna informasiya təhlükəsizliyi sahəsində texnoloji mədəniyyət, informasiya-psixoloji mədəniyyət, eləcə də hüquqi-etik mədəniyyətin komponentləri daxildir. Bu gün informasiya təhlükəsizliyi fərdin, cəmiyyətin və dövlətin yalnız maddi, iqtisadi, texnoloji və s. maraqlarının deyil, sosial-mənəvi, əxlaqi və digər qeyri-maddi dəyərlərinin də qorunmasını ifadə edir.(Mahmudova,2021)

Kibertəhlükəsizlik mədəniyyəti anlayışı təşkilatın işçi qüvvəsinin kibertəhlükəsizliklə bağlı münasibətinə, biliyinə, fərziyyələrinə, normalarına və dəyərlərinə aiddir.(CYBERSIGN, n.d.)

Bu mədəniyyət yalnız texniki biliklərə əsaslanmır, eyni zamanda insanların şüurlu, məsuliyyətli və ehtiyatlı davranmasını təmin edir. İnformasiya təhlükəsizliyi mədəniyyətinin məqsədi - insan amilindən doğan təhlükəsizlik zəifliklərini minimuma endirmək, və həm fərdi, həm də kollektiv səviyyədə təhlükəsiz rəqəmsal mühit yaratmaqdır.

Son illər ölkəmizdə kiberməkanda dövlət müstəqilliyinin, milli maraqların qorunması, informasiya təhlükəsizliyi sahəsində vahid dövlət siyasətinin təkmilləşdirilməsi və informasiya təhlükəsizliyinin texnoloji infrastruktur komponentlərinin yaradılması istiqamətində məqsədyönlü işlər aparılır. Ölkədə rəqəmsal transformasiya sürətləndikcə, kibertəhlükəsizlik və informasiya təhlükəsizliyi məsələləri daha da aktuallaşır. Dövlət və özəl sektor bu sahədə müxtəlif tədbirlər görsə də, hələ də bir sıra problemlər mövcuddur.

Vətən müharibəsinin ilk günlərindən kiberməkanda mümkün təxribatların və döyüş əməliyyatları ilə bağlı məlumatların sızmasının qarşısını almaq məqsədilə Azərbaycanın internet seqmentinin, həmçinin sosial şəbəkələr və digər elektron kommunikasiya platformaları vasitəsilə aparılan məlumat mübadiləsinin təhlükəsizliyinin təmin olunması istiqamətində kompleks tədbirlər həyata keçirilmişdir. İşğaldan azad olunmuş ərazilərdə müasir informasiya texnologiyalarına əsaslanan infrastrukturun yaradılması, “Ağıllı şəhər” və “Ağıllı kənd” konsepsiyalarının reallaşması regional sabitliyi və inkişafı şərtləndirən amillərdən biridir. Bu ərazilərdə dövlət və ictimai təhlükəsizliyin təmin olunması üçün mümkün terror-təxribat və digər nöqtələrin müəyyən edilməsi, çevik əks-tədbirlərin hazırlanması məqsədilə “big data”, “cloud”, “machine learning” texnologiyaları əsasında yaradılmış müvafiq həllərin tətbiqi nəzərdə tutulur.

Qlobal pandemiya şəraitində insanların, biznes dairələrinin, dövlət orqanlarının (qurumlarının) fəaliyyətinin əsas hissəsi kiberməkana keçmiş, müəssisə və təşkilatların bir qismi işçilərini məsafədən işə cəlb etmişdir. Əksər hallarda bu keçid sürətlə baş vermiş və istifadə olunan texnologiyaların və proqram təminatının təhlükəsizlik baxımından qiymətləndirilməsi lazımı qaydada aparılmamışdır. Məsafədən iş üçün tətbiq olunmuş proqram təminatının müxtəlifliyini və çoxsaylı istehsalçılara məxsus olduğunu nəzərə alaraq, fərdi məlumatların, kommersiya sirrinin və digər qorunan informasiyanın sızması təhlükəsi ötən illərlə müqayisədə dəfələrlə artmışdır. Bununla bağlı, qorunan informasiyanın mühafizəsi istiqamətində əlavə tədbirlərin həyata keçirilməsi zərurəti yaranmışdır.

Symantec-in (Broadcom) 2020-ci il üzrə qlobal kibertəhlükəsizlik hesabatına əsasən, COVID-19 pandemiyası dövründə fişinq kampaniyaları və zərərli proqram hücumları əhəmiyyətli dərəcədə artmışdır. Hücumçular insanların qorxu və qeyri-müəyyənlik hisslərindən istifadə edərək onları hədəfə almışdır.(Symantec, 2020)

Ümumiyyətlə, ölkədə kibercinayətlərlə mübarizə imkanlarının genişləndirilməsi üçün bir sıra mühüm hüquqi və təşkilati tədbirlər görülmüşdür. İnformasiya təhlükəsizliyi, habelə kibertəhlükəsizlik üzrə hüquqi bazanın təkmilləşdirilməsi məqsədilə Azərbaycan Respublikası aidiyyəti beynəlxalq konvensiya və proqramlara qoşulmuş, milli qanunvericilik bazası inkişaf etdirilmişdir.(Azərbaycan Respublikası Strategiyası, n.d)

Azərbaycanda informasiya təhlükəsizliyi mədəniyyətinin formalaşması və mövcud vəziyyət: Rəqəmsallaşma həyatımızın demək olar ki, bütün sahələrinə nüfuz etdikcə, informasiya təhlükəsizliyi

məsələsi də getdikcə daha vacib hala gəlir. Azərbaycanda bu sahədə müəyyən irəliləyişlər olsa da, ümumi mədəniyyətin formalaşması və mövcud vəziyyət bir sıra çətinliklərlə müşayiət olunur. Bu çətinlikləri bir neçə əsas istiqamətdə qiymətləndirmək mümkündür.

Maarifləndirmə və təhsil sahəsində çatışmazlıqlar : İnformasiya təhlükəsizliyi ilə bağlı ictimai maarifləndirmə hələ də geniş yayılmayıb. Məktəblərdə və universitetlərdə bu sahəyə aid dərslər ya çox məhduddur, ya da ümumiyyətlə mövcud deyil. Nəticədə, bir çox insanlar şəxsi məlumatlarını necə qoruyacaqlarını bilmirlər. Bu isə onları kibertəhlükələrə qarşı daha həssas edir.

Hüquqi və institusional boşluqlar: Qanunvericilik baxımından müəyyən addımlar atılsa da, kibertəhlükəsizlik sahəsində hələ də boşluqlar qalmaqdadır. Milli strategiya mövcuddur, lakin onun icrası praktikada tam effektiv deyil. Dövlət qurumları ilə özəl sektor arasında koordinasiya zəifdir və bu da vahid yanaşmanın formalaşmasına mane olur.

Sosial mediada risklər və fərdi səhlənkarlıq: Sosial şəbəkələrdə şəxsi məlumatların qorunması kifayət qədər zəifdir. İstifadəçilər çox zaman təhlükəsizlik tədbirlərinə laqeyd yanaşır, bu isə fırıldaqçılıq və məlumat oğurluğu hallarının artmasına səbəb olur. Bu cür səhlənkarlıq həm fərdi, həm də ümumi informasiya təhlükəsizliyi səviyyəsinə mənfi təsir göstərir.

Microsoft-un “Digital Defense Report 2023” sənədində sosial mühəndislik hücumlarının sürətlə artdığı vurğulanır.(Microsoft, 2023)

IBM-in 2023 hesabatına görə, məlumat sızmasının orta maliyyə itkisi 4,45 milyon ABŞ dolları təşkil edir.(IBM Security, 2023)

Azərbaycanda informasiya təhlükəsizliyi mədəniyyəti formalaşmaqda olsa da, hələ də bir sıra problemlər mövcuddur. Maarifləndirmə, hüquqi çərçivənin təkmilləşdirilməsi və texniki inkişaf bu sahədə əsas prioritetlərdən biridir. Dövlət və özəl sektorun birgə səyləri ilə bu sahədə daha güclü bir ekosistem yaratmaq mümkündür.

İnformasiya cəmiyyətinin inkişafı istiqamətində əsas problemlərdən biri dövlətin, cəmiyyətin və bu cəmiyyətin üzvü olan fərdlərin informasiya təhlükəsizliyinin təmin edilməsidir. Hər kəs informasiya təhlükəsizliyi sahəsində müəyyən zəruri biliklərə malik olmalıdır ki, get-gedə artan informasiya təhdidlərinə qarşı mübarizə apara bilsin, kibercinayətkarlar, kiberfırıldaqçılardan və s. özünü qoruya bilsin. Bunun üçün istifadəçilər ilk növbədə internetdə işləyərkən, müxtəlif elektron xidmətlərdən istifadə edərkən üzləşə biləcəkləri təhlükələr barədə məlumatlı olmalıdırlar.

İnformasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi müasir dövrdə böyük əhəmiyyət kəsb edir. Vətəndaşların və müxtəlif əhali qruplarının bu sahədə maarifləndirilməsi kiberhücumların, şəxsi məlumatların oğurlanmasının və dezinformasiyanın qarşısının alınmasına kömək edə bilər.(Mahmudova, 2022)

ENISA kibertəhlükəsizlik mədəniyyətinin formalaşmasında davranış modellərinin əhəmiyyətini xüsusi vurğulayır.(ITU, 2021)

ENISA-nın “Threat Landscape 2022” hesabatında qeyd olunur ki, Avropada kibertəhdidlərin sayı və mürəkkəbliyi artmaqda davam edir, xüsusilə ransomware, fişinq və DDoS hücumları əsas təhlükələr kimi ön plana çıxır; geosiyasi gərginliklər, o cümlədən Ukrayna müharibəsi, bu tendensiyaları daha da gücləndirmişdir.(ENISA, 2022)

Dünya ölkələri informasiya cəmiyyətinin inkişaf səviyyəsinə görə bir-birindən fərqlənsələr də, bütün ölkələrin informasiya təhlükəsizliyi problemləri, demək olar ki, oxşardır. Bu problemlərin həllinə yanaşmalar isə ölkənin mədəni səviyyəsindən və bu sahədəki milli hüquqi bazadan asılı olaraq fərqlənir. Ölkələrin əksəriyyəti vətəndaşların ilk növbədə informasiya məkanında qarşılaşdıqları təhlükələr və bu təhlükələrdən qorunma mexanizmləri barədə məlumatlandırılması, onların İTM-nin səviyyəsinin artırılması üçün müxtəlif tədbirlər həyata keçirirlər. Bu cür tədbirlərdə ümumi informasiya təhlükəsizliyi

məsələlərindən tutmuş, fərdi məlumatların qorunması, elektron imza, elektron şəxsiyyət vəsiqəsi, elektron tibbi xidmətlər, təhlükəsizlik risklərinin idarə edilməsi kimi konkret məsələlərə diqqət yetirilir.(Mahmudova, 2022)

Cədvəl 1. Kibertəlimlər keçirən beynəlxalq təşkilatların siyahısı

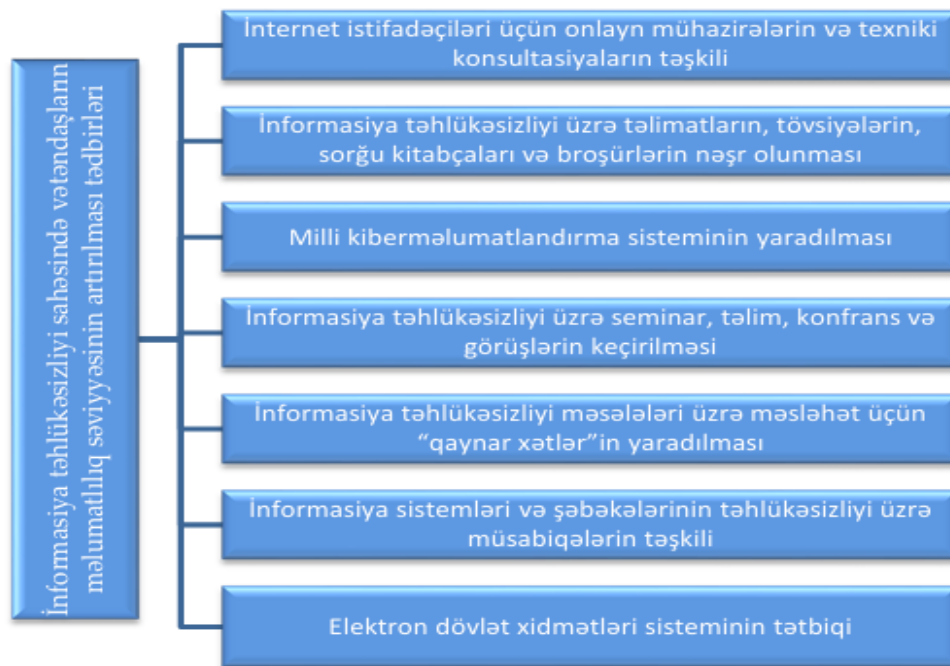
KİBER TƏLİMLƏR KEÇİRƏN TƏŞKİLATIN ADI	İNTERNET SAYTI
Asiya-Sakit okean İqtisadi Əməkdaşlıq Təşkilatı (Asia-Pacific Economic Cooperation, APEC)	www.apec.org
Cənub-Şərqi Asiya Dövlətləri Assosiasiyası (Association of SouthEast Asian Nations, ASEAN)	www.asean.org
Avropa Birliyi (European Union, EU)	www.europa.eu
Council of Europe (Avropa Şurası)	www.coe.int
Avropol (Europol)	www.europol.europa.eu
İnformasiya Təhlükəsizliyi İnsidentlərinə Reaksiya Komandalarının Forumu (Forum of Incident Response and Security Teams, FIRST)	www.first.org
Səkkizlər qrupu (Group of eight, G8)	www.g8russia.ru
Elektroteknika və Elektronika Mühəndisləri İnstitutu (Institute of Electrical and Electronics Engineers, IEEE)	www.ieee.org
Beynəlxalq Elektroteknika Komissiyası (International Electrotechnical Commission, IEC)	www.iec.ch
Beynəlxalq Standartlaşdırma Təşkilatı (International Organization for Standardization, ISO)	www.iso.org
Beynəlxalq Telekomunikasiya İttifaqı (International Telecommunication Union, ITU)	www.itu.int
İnternetdə domen adlarının və zonalarının verilməsini həyata keçirən qeyri-kommersiya təşkilatı (Internet Corporation for Assigned Names and Numbers, ICANN)	www.icann.org
İnternet mühəndisliyi üzrə işçi qrupu (Internet Engineering Task Force, IETF)	www.ietf.org/about/mission.html

İnternet İdarəçilik Forumu (Internet Governance Forum, IGF)	www.intgovforum.org/cms
---	--

Mənbə: İnformasiya cəmiyyəti problemləri, 2022, №1, 85-94

Vətəndaşların informasiya təhlükəsizliyi məsələləri üzrə məlumatlılıq səviyyəsinin yüksəldilməsi istiqamətində ölkələr tərəfindən müxtəlif tədbirlər həyata keçirilir.

Şəkil 1. Vətəndaşların məlumatlılıq səviyyəsinin artırılması tədbirləri



Mənbə: İnformasiya cəmiyyəti problemləri, 2022, №1, 85-94

Kaspersky-nin 2022 hesabatı göstərir ki, kibertəhlükəsizlik xərcləri qlobal miqyasda rekord səviyyəyə çatmışdır.(Kaspersky, 2022)

OECD-nin 2021 hesabatında milli kibertəhlükəsizlik strategiyalarının qlobal koordinasiyanın vacibliyi vurğulanır.(OECD, 2021)

İnformasiya təhlükəsizliyi mədəniyyətinin formalaşması bu gün qlobal miqyasda strateji əhəmiyyət daşıyan bir məsələdir. Müasir dövrdə rəqəmsal texnologiyaların sürətlə inkişaf etməsi fonunda bu sahədə uğurlu nümunələrin öyrənilməsi və tətbiqi vacibdir. Mənim fikrimcə, Estoniya və Yaponiya bu sahədə öyrənilməli iki önəmli model təqdim edir və onların təcrübəsi Azərbaycan üçün olduqca faydalı ola bilər. Estoniya: Rəqəmsal cəmiyyətin uğurlu modeli - Estoniya informasiya təhlükəsizliyi sahəsində aparıcı ölkələrdən biri kimi tanınır. Onların “e-Estonia” modeli rəqəmsal idarəetmə və kibertəhlükəsizlik sahəsində innovativ yanaşmaları ilə seçilir. Bu modeldə, elektron şəxsiyyət vəsiqəsi sistemi və blokçeyn texnologiyası vasitəsilə məlumatlar təhlükəsiz şəkildə qorunur; kibertəhlükəsizlik üzrə milli strategiya mövcuddur və bu strategiyaya uyğun təlim proqramları həyata keçirilir.

Yaponiya: Təhsil və texnologiya əsaslı yanaşma - Yaponiya isə informasiya təhlükəsizliyi mədəniyyətinin formalaşmasında daha çox təhsil və texnologiya yönümlü strategiyalara üstünlük verir. Bu ölkədə,

məktəblərdə və universitetlərdə kibertəhlükəsizlik mövzusunda dərslər keçirilir və gənc nəsilə bu sahəyə maraq artırılır; informasiya təhlükəsizliyi ilə bağlı milli qanunvericilik və normativ baza gücləndirilir; süni intellekt və digər innovativ texnologiyalar əsasında kibermüdafiə sistemləri tətbiq edilir. Yaponiyanın bu sahədəki təcrübəsi göstərir ki, informasiya təhlükəsizliyi yalnız texniki tədbirlərlə deyil, həm də maarifləndirmə və sosial yanaşmalarla gücləndirilə bilər.

Azərbaycan Respublikasının informasiya məkanının müasir təhdidlərdən qorunması milli təhlükəsizliyin əsas istiqamətlərindəndir. Ölkənin sosial-iqtisadi tərəqqisinin aparıcı qüvvəsi olan informasiya-kommunikasiya texnologiyalarının (bundan sonra – İKT) dinamik inkişafı bu sahədə mövcud olan və yeni yaranan risklərin təhlilinin aparılmasını, mühafizə obyektlərinin dəqiqləşdirilməsini, onların aid olduğu informasiya infrastrukturalarının funksional dayanıqlığını, bu infrastrukturardan istifadə edən subyektlərin hüquq və qanuni maraqlarını, fəaliyyətin davamlılığını təmin etmək üçün qabaqlayıcı və bərpaedici tədbirlərin müəyyənəndirilmiş səviyyədə görülməsini, informasiya təhlükəsizliyini idarəetmə alətlərinin davamlı təkmilləşdirilməsini şərtləndirir. (Azərbaycan Respublikası Strategiyası, n.d.)

Qloballaşan dünyada informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması istər milli, istərsə də beynəlxalq səviyyədə əsas məsələyə çevrilmişdir. Bu fəaliyyətdə insan, cəmiyyət və dövlət maraqlarının qorunması başlıca məqsəddir. Son zamanlar Azərbaycanın informasiya məkanına, o cümlədən onun tərkib hissələrinə (dövlət, özəl və qeyri-hökumət qurumlarının, fiziki şəxslərin sahib olduğu informasiya ehtiyatlarına və infrastrukturalarına, bu ehtiyatlarda olan məlumatların həyat boyu proseslərinə, həmin proseslər üçün istifadə olunan maddi və qeyri-maddi obyektlərə və onlar arasında əlaqələrə) qarşı texnoloji cəhətdən çoxşaxəli hücumlar genişlənməkdədir.

İnformasiya təhlükəsizliyi informasiya sahəsində milli təhlükəsizliyə təhdidləri müəyyən etmək, bu təhdidlərin istifadə edə biləcəyi zəifliklərin, boşluqların və təhdid nəticəsində yarana bilən fəsadların aradan qaldırılması və ya əvvəldən təyin edilmiş hədlərə qədər azaldılması üçün hüquqi, təşkilati, əməliyyat-axtarış, kəşfiyyat və əks-kəşfiyyat, elmi-texniki və təhsil, informasiya-təhlil, kommunikasiya, kadr təminatı, iqtisadi və digər sahələr üzrə tədbirləri əlaqələndirilmiş qaydada təşkil, icra, nəzarət və davamlı təkmilləşdirmək üçün qanunvericiliklə müəyyən edilən mühafizə üsulları və vasitələri ilə təmin edilir.

Kibertəhlükəsizlik sahəsində milli ekosistemin formalaşdırılması və inkişafı istiqamətində aparılmış əməli fəaliyyət ölkəmizin beynəlxalq reytinglərdə mövqeyinin ciddi şəkildə yaxşılaşdırılması ilə nəticələnmişdir. (Azərbaycan Respublikası Strategiyası, n.d.)

Azərbaycan Beynəlxalq Telekomunikasiya İttifaqının tərtib etdiyi “Qlobal kibertəhlükəsizlik indeksi 2020” (Global Cybersecurity Index, GCI) reytingində mövqeyini 15 pillə yaxşılaşdıraraq, 194 ölkə arasında 89.31 xal ilə 40-cı yerdə qərarlaşmışdır. (ITU, 2021). Qlobal hesabatlarda da kibertəhlükəsizlik dövlətlərin prioritetləri arasında yer alır, məsələn, Dünya İqtisadi Forumunun “Qlobal Risklər Hesabatı”nda kibertəhlükəsizlik əsas beş təhlükədən biri kimi göstərilir. (World Economic Forum, 2024)

Azərbaycan informasiya təhlükəsizliyi sahəsində beynəlxalq təcrübədən faydalana bilər:

- Rəqəmsal hökumət və e-İD sistemlərinin gücləndirilməsi.
- Kibertəhlükəsizlik üzrə maarifləndirmə kampaniyaları və təlimlər.
- Milli kibertəhlükəsizlik strategiyasının inkişaf etdirilməsi.
- Hökumət və özəl sektor arasında əməkdaşlığın genişləndirilməsi.

İnformasiya təhlükəsizliyi mədəniyyətinin cəmiyyətdə formalaşması ilə bağlı real nümunələr müxtəlif sahələrdə müşahidə olunur. Məsələn:

ABŞ - Şirkətlərdə Kibertəhlükəsizlik Mədəniyyəti: Böyük korporasiyalar, məsələn, Google və Microsoft, kibertəhlükəsizlik mədəniyyətini inkişaf etdirmək üçün işçilərinə mütəmadi təlimlər keçirir. Bu şirkətlər kibertəhlükələrə qarşı mübarizə aparmaq üçün güclü təhlükəsizlik protokolları tətbiq edir və işçilərin məlumat təhlükəsizliyi qaydalarına riayət etməsini təmin edirlər.

ABŞ-da tətbiq edilən NIST-in “Framework for Improving Critical Infrastructure Cybersecurity” sənədi təşkilatlara informasiya təhlükəsizliyi risklərini idarə etmək və kritik infrastrukturun müdafiəsini gücləndirmək üçün strukturlaşdırılmış yanaşma təqdim edir.(NIST,2018)

Avropa ittifaqı-GDPR Qaydaları: Avropa İttifaqı şəxsi məlumatların qorunmasını gücləndirmək üçün Ümumi Məlumatların Qorunması Qaydaları (GDPR) tətbiq edib. Bu qaydalar şirkətləri və fərdləri məlumat təhlükəsizliyi mədəniyyətini inkişaf etdirməyə təşviq edir və şəxsi məlumatların qorunmasını təmin edir.

Sinqapur - Mill Kibertəhlükəsizlik Strategiyası: Sinqapur hökuməti kibertəhlükəsizlik sahəsində ciddi tədbirlər görərək milli strategiya hazırlayıb. Bu strategiya çərçivəsində dövlət qurumları və özəl sektor kibertəhlükəsizlik mədəniyyətini gücləndirmək üçün birgə fəaliyyət göstərir.

Böyük Britaniya - Kibertəhlükəsizlik Maarifləndirmə Kampaniyaları: Böyük Britaniyada kibertəhlükəsizlik sahəsində maarifləndirmə kampaniyaları geniş yayılıb. Xüsusilə “Cyber Aware” təşəbbüsü fərdləri və biznesləri kibertəhlükələrə qarşı mübarizə aparmağa təşviq edir.

Bu nümunələr göstərir ki, informasiya təhlükəsizliyi mədəniyyəti cəmiyyətin müxtəlif sahələrində formalaşma bilər ya onun inkişafı üçün maarifləndirmə, qanunvericilik və texnoloji hallar vacibdir.

“Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası” dövlətin, cəmiyyətin və insanların müasir İKT-dən təhlükəsiz istifadəsinin təmin edilməsi üçün milli informasiya təhlükəsizliyi səviyyəsinin yüksəldilməsinə, dövlət və özəl şəbəkələrin, kritik informasiya infrastrukturlarının təhlükəsizliyinin təmin olunmasına aid tədbirlərin müəyyənləşdirilməsinin və həyata keçirilməsinin təşkilinə, həmçinin fərdi məlumatların mühafizəsinə, Azərbaycan Respublikasının Konstitusiyası ilə təsbit edilmiş insan hüquq və azadlıqlarına riayət edilməsinə daha əlverişli şəraitin yaradılmasına xidmət edir.(Azərbaycan Respublikası Strategiyası, n.d.)

Azərbaycan Respublikası Prezidentinin 2018-ci il 29 mart tarixli 3851 nömrəli Sərəncamına uyğun olaraq yaradılmış İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyası Azərbaycan Respublikasında informasiya məkanının təhlükəsizliyinin təmin edilməsi, dövlət və cəmiyyət üçün xüsusi əhəmiyyət kəsb edən infrastruktur obyektlərinin informasiya sistemləri və ehtiyatlarının kiberhücumlardan qorunması, təhdidlərin qabaqlanması, qarşısının alınması və araşdırılması sahəsində fəaliyyət göstərən dövlət qurumlarının işinin əlaqələndirilməsini təşkil edir.(İTKK, n.d.)

Müasir dövrdə informasiya təhlükəsizliyi siyasətləri yalnız texnoloji tədbirlərlə məhdudlaşmır. Bu sahədə effektivlik üçün hüquqi və idarəetmə mexanizmlərinin möhkəmləndirilməsi zəruridir. Harvard Kennedy School-un Belfer Center-in araşdırmalarına görə, kibertəhlükəsizlik sahəsində effektivlik yalnız texnoloji tədbirlərlə deyil, həm də güclü idarəetmə və hüquqi-normativ çərçivələrin mövcudluğu ilə təmin olunur.(Harvard Kennedy School – Belfer Center, 2021)

NƏTİCƏ VƏ TÖVSIYƏLƏR:

İnformasiya təhlükəsizliyi mədəniyyətinin formalaşması yalnız texniki tədbirlərlə məhdudlaşmır; bu proses həm hüquqi, həm sosial, həm də texnoloji aspektləri əhatə etməlidir. Öz təhlilimə əsaslanaraq, bu sahədə bir neçə əsas istiqamətdə konkret addımların atılmasının vacib olduğunu düşünürəm:

İlk növbədə, kibertəhlükəsizlik sahəsində maarifləndirmə işləri genişləndirilməlidir. Məktəblərdə və universitetlərdə bu mövzuya dair kursların sayının artırılması, gənc nəsildə informasiya təhlükəsizliyi mədəniyyətinin formalaşmasına ciddi töhfə verə bilər. Eyni zamanda, dövlət və özəl sektorun birgə şəkildə

maarifləndirmə kampaniyaları keçirməsi, fərdi istifadəçilər üçün təlimlərin təşkili bu sahədə ümumi bilik səviyyəsini yüksəldəcək.

Mövcud qanunvericilik bazası kibertəhlükəsizlik sahəsində daha da təkmilləşdirilməlidir. Yeni qanunvericilik təşəbbüslərinin hazırlanması və qəbul edilməsi bu sahədə hüquqi boşluqları aradan qaldıra bilər. Eyni zamanda, dövlət və özəl sektor arasında əməkdaşlığın gücləndirilməsi və milli kibertəhlükəsizlik ekosisteminin inkişaf etdirilməsi vacibdir.

Estoniya, Yaponiya və digər qabaqcıl ölkələrin kibertəhlükəsizlik strategiyaları öyrənilməli və yerli kontekstə uyğun şəkildə tətbiq edilməlidir. Bu modellərin araşdırılması Azərbaycanda daha effektiv və dayanıqlı sistemlərin qurulmasına imkan verə bilər.

Kibertəhlükəsizlik sahəsində innovativ həllərin inkişaf etdirilməsi üçün dövlət və özəl sektor arasında daha sıx əməkdaşlıq vacibdir. Birgə layihələrin həyata keçirilməsi həm texnoloji yeniliklərin tətbiqini sürətləndirir, həm də resursların daha səmərəli istifadəsinə şərait yaradır.

Süni intellekt və avtomatlaşdırılmış təhlükəsizlik sistemlərinin tətbiqi kibertəhlükələrə qarşı daha çevik və effektiv müdafiə təmin edə bilər. Eyni zamanda, kibertəhlükəsizlik üzrə milli reyestrin yaradılması və qabaqlayıcı tədbirlərin gücləndirilməsi bu sahədə risklərin idarə olunmasını daha sistemli hala gətirir.

MIT Technology Review-un 2022-ci il araşdırmalarına əsasən, gələcəyin kibertəhlükəsizlik modeli süni intellektin imkanlarına və istifadəçi davranışlarının analizinə əsaslanacaq, bu da təhlükələrin daha sürətli və dəqiq aşkarlanmasını təmin edəcək. (MIT Technology Review, 2022)

ISO/IEC 27002:2022 standartı informasiya təhlükəsizliyinin idarə olunması üçün strukturlaşdırılmış və müasir nəzarət mexanizmləri təqdim edir. Bu mexanizmlər təşkilatlara risklərin idarə olunmasında və məlumatların qorunmasında sistemli yanaşma təmin edir. (ISO, 2022)

Müasir dövrdə informasiya təhlükəsizliyi təkcə texnoloji tədbirlərlə məhdudlaşmır, bu sahədə uğur əldə etmək üçün cəmiyyətin hər bir üzvündə informasiya təhlükəsizliyi mədəniyyətinin formalaşması zəruridir. Məqalədə göstəriləndiyi kimi, rəqəmsal texnologiyaların inkişafı və internetin geniş yayılması ilə yanaşı, fərdi və institusional səviyyədə məlumatların qorunması məsələsi daha da aktuallaşmışdır. Azərbaycanda bu istiqamətdə mühüm addımlar atılsa da, maarifləndirmə, hüquqi bazanın təkmilləşdirilməsi, texnoloji infrastrukturun gücləndirilməsi və dövlət-özəl sektor əməkdaşlığı sahəsində hələ də çatışmazlıqlar qalmaqdadır.

PwC-nin 2022-ci il Global Digital Trust Insights sorğusuna əsasən, kibertəhlükəsizlik sahəsində dövlət və özəl sektor arasında əməkdaşlıq etimadın formalaşması və risklərin daha effektiv idarə olunması üçün mühüm rol oynayır. (PwC, 2022)

İnformasiya təhlükəsizliyi mədəniyyətinin inkişafı üçün təhsil sistemində kibertəhlükəsizlik üzrə tədrisin genişləndirilməsi, əhəlinin müxtəlif təbəqələri üçün maarifləndirici kampaniyaların təşkili, beynəlxalq təcrübədən faydalanmaq və qabaqlayıcı təhlükəsizlik tədbirlərinin görülməsi zəruridir. Bu istiqamətdə dövlət və özəl sektorun qarşılıqlı əməkdaşlığı ilə informasiya təhlükəsizliyinə dair güclü və dayanıqlı bir mədəniyyətin formalaşdırılması mümkündür. Yalnız bu halda informasiya cəmiyyətində vətəndaşların hüquq və maraqları effektiv şəkildə qoruna bilər.

Accenture tədqiqatına əsasən, kibermüdafiə qabiliyyəti yüksək olan təşkilatlar kiberhücumlara daha az məruz qalır. (Accenture, 2021)

ƏDƏBİYYAT SİYAHISI

1. Accenture. *State of Cybersecurity Resilience 2021*. Accenture, 2021.

[State of Cybersecurity Report 2021 | 4th Annual Report | Accenture](#)

2. Azərbaycan Respublikasının İnformasiya Təhlükəsizliyi və Kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası

<https://www.itkk.gov.az/az/strategiya/strategiya-haqqinda>

3. CYBERSIGN. *Kibertəhlükəsizlik mədəniyyəti nədir?*

[CYBERSIGN - Secure Future](#)

4. European Union Agency for Cybersecurity. (2022). *ENISA Threat Landscape 2022*. ENISA.

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

5. Harvard Kennedy School – Belfer Center for Science and International Affairs. (2021). *Cybersecurity and Digital Governance*. Harvard University.

[Cyber Project | The Belfer Center for Science and International Affairs](#)

6. . IBM Security. *Cost of a Data Breach Report 2023*. IBM, 2023.

<https://www.securityhq.com/reports/cost-of-a-data-breach-report-2023/>

7. İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyasının Strategiyası

[İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyası haqqında Əsasnamə » Azərbaycan Prezidentinin Rəsmi internet sahifəsi](#)

8. ISO/IEC 27002:2022. *Information Security, Cybersecurity and Privacy Protection — Information Security Controls*. International Organization for Standardization, 2022.

9. ITU. *Global Cybersecurity Index 2020*. International Telecommunication Union, 2021.

[Azerbaijan significantly improved its cybersecurity index in international ranking / News / Media - Mincom](#)

10. Kaspersky. *IT Security Economics 2022*. Kaspersky, 2022.

[kaspersky IT Security economy Report 2205 final](#)

11. Mahmudova R.Ş. (2021). Fərdin və cəmiyyətin informasiya təhlükəsizliyi mədəniyyətinin bəzi aspektləri haqqında

[ON SOME ASPECTS OF THE CULTURE OF INFORMATION SECURITY OF AN INDIVIDUAL AND SOCIETY.pdf](#)

12. Mahmudova Rəsmiyyə Ş.(2022). Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində beynəlxalq təcrübənin analizi

[ANALYSIS OF INTERNATIONAL EXPERIENCE IN THE FORMATION OF A CULTURE OF INFORMATION SECURITY IN SOCIETY.pdf](#)

13. Microsoft. *Digital Defense Report 2023*. Microsoft, 2023.

https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MDDR_FINAL_2023_1004.pdf

14. . MIT Technology Review. (2022). *The Future of Cybersecurity*.

[What's next in cybersecurity | MIT Technology Review](#)

15. National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST.

[Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1](#)

16. OECD. *Cybersecurity Policy Making at a Turning Point*. OECD Publishing, 2021.

[Cybersecurity Policy Making at a Turning Point | OECD](#)

17. PwC. *Global Digital Trust Insights 2022*. PwC, 2022.

[The C-Suite guide to simplifying for cyber readiness, today and tomorrow: PwC](#)

18. Symantec (Broadcom). (2020). *Internet Security Threat Report 2020*. Symantec.

[Symantec Security Summary - June 2020 | SECURITY.COM](#)

19. World Bank. *Cybersecurity: A Foundation for Digital Transformation*, 2023

<https://www.worldbank.org/en/topic/digital/brief/cybersecurity>

20. . World Economic Forum. *Global Risks Report 2024*. Geneva: WEF, 2024.

[Cyber Insecurity and Misinformation Top WEF Global Risk List - Infosecurity Magazine](#)